MediaSec Technologies
The Media Security Company

FIFA World Cup 2006 Venue-Access Security Solution

stolen badges performed as a function of the Reader's firmware. The blacklist was updated and synched nightly with Readers.

- Venue-entry security activities were assisted by technology-supported administrative procedures including:
  - Maintenance and nightly synching of the 'blacklist'
  - Data review and auditing to determine:
    - Improved reader performance and practices
    - Identification of potential fraudulent badge counterfeiting patterns
  - Reader maintenance activities

Solution Performance
As reported in a debriefing meeting, Accreditation indicated the 2006 FIFA World Cup events were the most secure international sports event managed by FIFA to date. It became clearly evident that without the use of automated verification with the CR2, it was not possible to enforce all the rules and individual access scenarios for each of the 150,000 accredited persons. The use of the Data Matrix and CDP codes fully achieved the goals of Accreditation.

Several counterfeit badges were identified and confiscated. Some authentic looking identification badges had been sold for €1,000 each. Procedural errors in applying the defined access control scenarios were routinely detected. In addition, quite a few volunteers and employees were denied entrance to unauthorized venues and areas, or at times when they were not allowed. The 'hidden' digital security came as quite a surprise for all counterfeiters and abusers as they were not aware of this additional level of security.

"The reliable deployment of the bar code readers was crucial for successful security access control during the World Cup 2006. We received very good and effective support throughout the planning, implementation and operation phases."
– Albert Hilber, Information Technology Project Manager for FIFA World Cup 2006 - Accreditation Department

MediaSec Contact:
Susann Koch
Marketing & Communications
MediaSec Technologies GmbH
Phone +49 (0) 201 4375 254
Fax +49 (0) 201 4375 277
skoch@mediasec.de
www.mediasec.de
Code Contact:
Kerri Humpherys
Director, Marketing Communications
Code Corporation
801 495 2200 x. 210 - office
801 859 2913 - cell
kerri.humpherys@codecorp.com
www.codecorp.com

PEPPERL+FUCHS code

Case Study - FIFA World Cup 2006

Case Study - FIFA World Cup 2006

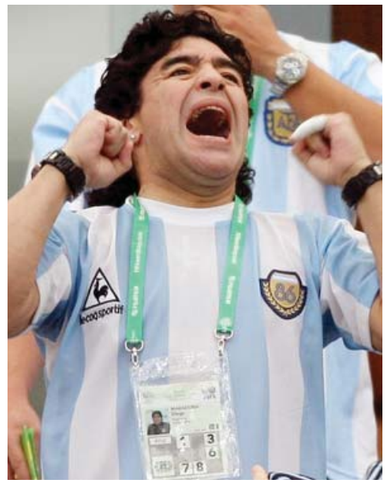
MediaSec Technologies
The Media Security Company

code
PEPPERL+FUCHS

Case Study -- An Integrated Venue-Access Security Solution for FIFA World Cup 2006

Germany was host to the 2006 FIFA World Cup Tournament for four short weeks in June and July. An estimated thirty billion people watched as 32 teams battled 'on the pitch' in 64 separate matches, while 147 goals were scored and each team vied for first-place position. Over 3,300,000 fans watched the games 'live' in 12 separate stadiums. Along with all the spectators, a staggering 150,000 non-ticket holders had need to gain entrance to the same venues, at varying times, in differing venue areas, in order to manage or participate in events or to provide on-going services to venue locations. How was venue entrance managed efficiently and how was security implemented?

The security requirements for hosting the games were daunting. As part of the Local Organizing Committee (LOC) for the Tournament, the Accreditation Department (Accreditation) was tasked with ensuring any person present in any specific area of any venue at any given time had a credible reason to be present. It was a widely held belief that in the past, vendors, employees and the large number of volunteers had taken advantage of 'entrance-rights' to venues. Many people had made so-called job-related visits during matches, watching the event while presumably on the job. Others exploited advantages of venue entry, entering areas normally not available to them. Additionally, with the current level of increased global security, team member safety was a consideration as well as the safety of attendees, service providers and the media. All these concerns prompted Accreditation to explore additional security measures concerning venue entry.



Diego Maradona – 2006 VIP guest and retired Argentine player wearing venue-access identification badge

Security Technology Search
Accreditation's goal was to augment current security levels to ensure appropriate venue entrance for vendors, employees, VIP guests, media, volunteers, emergency medical personnel, police, soccer team players and their family members. All non-ticketed personnel entrance scenarios were under scrutiny.

A search was initiated for a technology system that could be used at security checkpoints to further validate individual entry considerations. At first, Accreditation was considering using RFID technology; however, that solution proved to be too expensive with little portability and not much flexibility in use. Also, there were no reliable portable RFID readers on the market.

Accreditation was looking for ways to protect 'access control' information. Two goals emerged as they searched for a solution:

1. Control entry of non-ticketed personnel at venues, ensuring approved attendance at World Cup events; and
2. Deny entrance to non-ticket holders with stolen/fraudulent badges or if the individual did not have a credible reason to be allowed entry.

Accreditation's technology search lead them to MediaSec Technologies GmbH (MediaSec), located in their own native country of Germany. MediaSec offered Accreditation several very important solutions:

1. Encrypted bar codes to protect the access control information;
2. Copy Detection Pattern (CDP) – MediaSec's proprietary symbology that would authenticate individual identification badges;
3. Code's highly developed Code Reader 2.0 (CR2) that reads and decodes any bar code

MediaSec Technologies
The Media Security Company

type with Dynamic Optimization Technology, a proprietary bar code reading performance enhancement tool that quickly adapts Reader performance; and,

4. Software to manage and support venue security process operations, auditing and counterfeit detection of badges.

The bar code symbology selected to protect the access control information was a two-dimensional

> "When MediaSec was first approached by Accreditation, I realized we were being given a rare opportunity to test our technology on a large scale. Our security technology is unchallenged in the marketplace and clearly we had a viable technology-based answer to the need."
>
> – Dr. Jan Vorbrüggen, Manager of Business Development at MediaSec

Data Matrix code. This code could hold all the specific information for venues, dates and times the badge holder would be allowed entrance.

MediaSec's proprietary digital security technology – CDP – is designed specifically to limit counterfeiting or copying practices. A CDP symbol has the appearance of a two-dimensional bar code with intentional information loss. The fragmented symbol is virtually impossible to duplicate, ultimately providing the desired protection against counterfeiting. In addition, the process of encoding and decoding CDP can incorporate the use of a secret key code, adding an additional layer of security to the identification process. CDP provided the counterfeiting protection Accreditation was seeking.

These two codes would be read and decoded by the CR2. Uniquely developed CR2 firmware and PC-based computer software would accomplish an electronic review against a 'blacklist' of known fraudulent or stolen identification badges and an authenticity check of the CDP code.

After a test was completed of the barcode access control technology at an unrelated athletic event, Accreditation was satisfied that an appropriate solution had been identified. Information was exchanged and the project was initiated.

Partnered Solution

MediaSec is a value-added reseller for Pepperl+Fuchs (P+F) – a leading developer and manufacturer of electronic sensors and components for the global automation market. P+F is a world-wide distributor of Code Products including the CR2, the wireless bar code Reader able to read and decode MediaSec's proprietary CPD symbology as well as the Data Matrix codes used in the World Cup solution. All three parties worked together to provide a flexible and integrated hardware/software solution for Accreditation.

MediaSec solutions included:

- Tailored Reader Firmware (developed using Code's Software Development Kit) integrated with current Code Reader Firmware to accomplish the following:
  - Reading, analysis and authentication of CDP to verify badge authenticity
  - Reading and decrypting of Data Matrix bar code to manage access control
  - Comparison of badge information to 'blacklist' to identify counterfeit or stolen badges
- PC-based process management software, to manage:
  - Configuration of Readers indicating authorizations for venue, date and time
  - Blacklist maintenance
  - Check-in/check-out process of Readers to security personnel
  - Firmware updates to multiple Readers at once
  - Verification at completion of Reader updates
- Reader Optic 'nose' to optimize Reader position and CDP code magnification

Code products (as sold and supported by P+F) included:

- 300 CR2 Bar code Readers, Handles and Batteries
- 27 Two-Bay Battery Chargers
- Code Reader Firmware enabling reading and decrypting of Data Matrix and CDP bar codes

Venue Entry Process

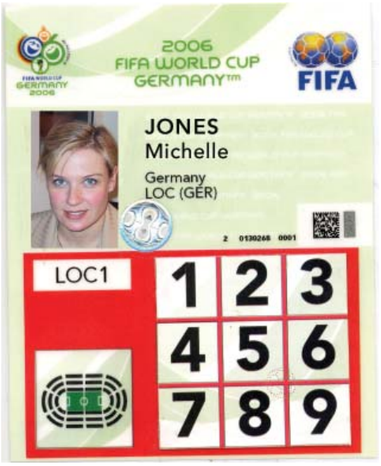
The venue entry process at security check points for the 2006 FIFA World Cup Tournament included several major components:

code PEPPERL+FUCHS

MediaSec Technologies
The Media Security Company

- An individual requesting venue entrance with an identification badge containing:
  - Official event branding
  - Badge holder's name
  - Color digital photo
  - Data Matrix code containing information regarding the dates, times, venues and areas of access for that individual
  - CDP code used to authenticate the badge
  - 'Large' numbers to indicate approved venue

Venue-access identification badge issued to all non-ticket holders



Timeline

January 2005	Initial meeting of MediaSec and Accreditation
January 2005	Specification developed for Data Matrix code
April 2005	Data Matrix code testing
May 2005	Accreditation delivers 'Letter of Intent'
May 2005	PC Software/Reader Firmware development
May 2005	Delivery of 'beta' Data Matrix code
June 2005	Successful test of unencrypted Data Matrix code
October 2005	MediaSec delivers Proposal (including CDP)
November 2005	Proposal accepted
November 2005	Software/Firmware integration
December 2005	Successful test of CDP and logistics
December–April 2006	Badge production testing
March 2006	Qualification review of hardware/software and processes
May 2006	Badge & Reader deployment begins at International Broadcast Center in Munich
May–June 2006	Deployed 300 CR2s to 14 locations
June–July 2006	World Cup Tournament: On-going support and on-site training

area access
- Stadium icons identifying approved venues
- Additional physical security measures (e.g., hologram)

Note: To obtain an identification badge, each person had to register on-line and provide the requested information to accomplish a security clearance check. The individual would be notified by email if the security clearance was successful. The person then needed to report to one of several security offices at identified venues to obtain an identification badge.

- A Security guard (with a CR2 Bar Code Reader) who:
  - Visually compared the digital photo on the identification badge to the person
  - Visually reviewed 'large numbers' and stadium icons on identification badge indicating approved venue access
  - Used the CR2 to read the Data Matrix Code and CDP code and waited for visual/audible verification before allowing

> "As partners, all three businesses worked together to provide a very unique solution for Accreditation. The integration of the hardware and software solutions utilizing several proprietary technologies was very successful."
>
> – George Powell, President and CEO of Code Corporation

entrance:
- Green LED light & two short beeps = Access permitted
- Red LED light & one long beep = Access denied
- Yellow LED light & one short beep = Scan second badge issued to service providers/employees only and review Green or Red LEDs (see previous)

Note: Verification also included a check against a 'blacklist' of known fraudulent or

PEPPERL+FUCHS code

Case Study - FIFA World Cup 2006